

Odpowiedzi na pytania do RFI nr BST-P6/076/41/2022

dot. dostarczenia licencji, świadczenia usługi wraz ze wsparciem i szkoleniem, opartej na rozwiązaniu typu PAM (Privileged Access Management) umożliwiającym monitorowanie i nagrywanie sesji zdalnych

1. System będący w ofercie naszej firmy jest licencjonowany na liczbę administratorów systemu, którzy mogą zarządzać jego działaniem, dodawać nowe zasoby oraz udostępniać je dalej użytkownikom (nie ma odgórnych limitów na użytkowników jednoczesnych). Ilu administratorów w Państwa przypadku przyjąć do wyceny rozwiązania?

Odp. 8 administratorów

2. Jaki model licencji Państwa interesuje – subskrypcyjny na 24 i 36 m-cy czy wieczysty ze wsparciem na 24 i 36 m-cy?

Odp. Zamawiający wymaga przedstawienia informacji cenowej obejmującej zapewnienie udzielenia licencji do rozwiązania wykorzystywanego do celów komercyjnych w następujących modelach:

- licencje wieczyste
- licencje na okres 24 miesięcy
- licencje na okres 36 miesięcy

3. Czy jeśli niektóre wymagania nie są spełniane – oczekują też Państwo tego typu ofert, z zaznaczeniem, które to wymogi?

Odp. W przypadku, jeżeli oferowane rozwiązanie nie spełnia wymagań określonych przez Zamawiającego, prosimy w informacji cenowej określić przyczyny w polu uwagi.

4. Czy informacja cenowa ma uwzględniać posiadane już przez Zamawiającego licencje PAM czy zapytanie dotyczy całkowicie odrębnej infrastruktury i nie należy kosztów odnowienia wsparcia dla posiadanych licencji uwzględniać w informacji cenowej?

Odp. Zamawiający dopuszcza przedstawienie informacji cenowej obejmującej rozbudowę obecnie wykorzystywanego u Zamawiającego rozwiązania PAM o:

- dostarczenie sprzętu wraz z zapewnieniem wsparcia producenta
- odnowienie wsparcia producenta dla posiadanych przez Zamawiającego licencji

5. Ile źródeł ma być monitorowanych?

Odp. „4.37. Rozwiązanie posiada min. 2 interfejsy sieciowe z możliwością rozszerzenia do obsługi min. 50 jednoczesnych sesji graficznych”

6. Ilu użytkowników uprzywilejowanych ma mieć możliwość korzystania z systemu?

Odp. Jw

7. Czy licencje systemu mają być przedstawione w formie wieczystej czy subskrypcyjnej, na okres 1 roku czy 3 lat?

Odp. Zamawiający wymaga przedstawienia informacji cenowej obejmującej zapewnienie udzielenia licencji do rozwiązania wykorzystywanego do celów komercyjnych w następujących modelach:

- licencje wieczyste
- licencje na okres 24 miesięcy
- licencje na okres 36 miesięcy

8. Na jakich funkcjonalnościach systemu Państwu zależy: monitorowanie sesji, nagrywanie, podwójna autentykacja, etc.

Odp. Funkcjonalności wskazane w pytaniu.

9. Czy w ramach wdrożenia planowane jest również uruchomienie automatycznej rotacji poświadczeń dla kont uprzywilejowanych chronionych przez system PAM? (Jest to zalecane podejście). Jeśli tak, bardzo proszę o informację na temat przybliżonej ilości kont z podziałem na:

- a. Konta domenowe (należące do administratorów)

Odp. do 8 kont administratorów

- b. Konta lokalne Windows

Odp. do 8 kont administratorów

- c. Konta lokalne *NIX

Odp. 8 kont administratorów

- d. Inne (np. VMWare ESXi root) jeżeli wchodzi w zakres wdrożenia

Odp. do 4 kont administratorów

10. Czy w ramach „virtual appliance” Zamawiający dopuszcza instalację oprogramowania systemu PAM na wcześniej przygotowanych przez Zamawiającego serwerach z odpowiednim systemem operacyjnym zgodnie z przygotowaną przez dostawcę specyfikacją?

Odp. Zamawiający dopuszcza takie rozwiązanie

11. Wymaganie 5.10 – Migracja konfiguracji z istniejącego systemu PAM. W jakim zakresie wymagane jest wsparcie dostawcy? Jeżeli, wymagane jest wsparcie w zakresie migracji kont uprzywilejowanych do nowego systemu to jaka jest przybliżona ilość kont uprzywilejowanych?

Odp. Dotyczy przeniesienia pełnej funkcjonalności obecnego rozwiązania na nową platformę

12. Czy z rozwiązania PAM będą korzystać również pracownicy zewnętrzeni np. dostawcy?
Jeśli tak, proszę o podanie liczby użytkowników systemu PAM z podziałem na pracowników wewnętrznych oraz pracowników zewnętrznych

Odp. Tak

13. Pytanie dotyczące przedmiotu zapytania oraz terminy wdrożenia usługi do 30 dni roboczych – czy wdrożenie usługi w wymienionym terminie będzie obowiązywało od daty przygotowania przez Zamawiającego wymaganej przez system PAM infrastruktury?

Odp. Czas liczony od przyjęcia harmonogramu uzgodnionego pomiędzy Zamawiającym a Dostawcą

14. Kiedy planujecie Państwo zakup i uruchomienie rozwiązania zgodnie z przedmiotowym zapytaniem RFI?

Odp. Do końca 2022 roku.

15. - Rozwiązanie umożliwia tagowanie i komentowanie przeglądanych sesji;
Czy zamawiający dopuszcza rozwiązanie nie posiadające możliwości tagowania sesji ale z możliwością ich audytu oraz komentowania?

Odp. Zamawiający dopuszcza takie rozwiązanie

16. - Rozwiązanie umożliwia dołączenie się administratora do sesji telnet, SSH, RDP, VNC z poziomu przeglądarki (np. dla wprowadzenia hasła, wpisanie polecenia systemowego);
Czy zamawiający dopuszcza rozwiązanie pozwalające na podgląd aktywnej sesji oraz możliwość jej zatrzymania lub wstrzymania bez możliwości interakcji?

Odp. Zamawiający dopuszcza bez możliwości interakcji.

17. - Liczba licencji opcjonalnie 300, 400 lub 500 na użytkowników jednoczesnych oraz serwery „Czy zamawiający poprzez użytkowników jednoczesnych rozumie równoczesne sesje czy dodanych użytkowników w systemie?”
„W przypadku, gdy produkt licencjonowany jest przez liczbę dodanych w systemie użytkowników (zamiast równoczesnych sesji), jaką liczbę użytkowników wymaga zamawiający?”

Odp. Zamawiający pyta na okoliczność ceny zależnie od liczby monitorowanych serwerów.

18. 6.1. Szkolenia administratorów PAM w liczbie 4, będą przeprowadzone w terminie uzgodnionym z PKP Intercity S.A.;

6.2. Szkolenia odbędą się w autoryzowanym ośrodku producenta oprogramowania i zakończą się

uzyskaniem niezbędnych certyfikatów dla administratorów Zamawiającego;

6.3. Zakres szkolenia musi uwzględniać:

6.3.1. Ogólną architekturę systemu PAM;

6.3.2. Bezpieczeństwo systemu PAM

6.3.3. Konfigurację kont systemów docelowych w systemie PAM

- 6.3.4. Zarządzanie użytkownikami w systemie PAM i integracja z innymi mechanizmami
- 6.3.5. uwierzytelniania i autoryzacji
- 6.3.6. Polityki złożoności hasła, harmonogram zmian haseł, walidacja poprawności zmiany hasła
- 6.3.7. Zarządzanie sesjami w systemie PAM
- 6.3.8. Zarządzanie schematami wnioskowania i akceptacji dostępu do hasła i/lub sesji w systemie PAM
- 6.3.9. Auditing i raportowanie w systemie PAM.
- 6.3.10. Certyfikat ukończenia szkolenia w zakresie administrowania PAM.

Czy zamawiający dopuszcza szkolenie w ośrodku szkoleniowym dystrybutora lub w siedzibie zamawiającego?

Odp. Zamawiający prosi o wskazanie kosztów szkoleń w wariantach:

- w autoryzowanym ośrodku producenta oprogramowania
- w ośrodku szkoleniowym dystrybutora lub
- w siedzibie Zamawiającego

19. W pkt 4.34 Zamawiający wymaga aby: System musi być certyfikowany na zgodność ze standardem FIPS 140 Level 2 (lub wyższym) lub 0 (lub wyższym);. Rzeczony standard jest wymogiem bezpieczeństwa amerykańskiego rządu w procesie zatwierdzania modułów kryptograficznych. Przedmiot zamówienia dotyczy informacji cenowej systemu klasy PAM, gdzie nie mają zastosowania wymagania dla modułów kryptograficznych. Oferowany przez Oferenta PAM spełnia wszystkie pozostałe wymagania funkcjonalne wymagane przez Zamawiającego, które adekwatnie do przedmiotu zapytania są oczekiwane dla systemów tej klasy. Wymaganie zatem wydają się być nad wymiarowym, a w szczególności ograniczającym konkurencję. Bazując na swojej najlepszej wiedzy oferent nie zna systemu typu PAM, który spełniałby niniejsze wymaganie, dlatego też czy Zamawiający może zrezygnować z niniejszego wymagania na rzecz oświadczenia producenta o spełnianiu tych norm oraz standardów dotyczących produkcji oprogramowania?

Odp. Zamawiający dopuszcza oświadczenia producenta z możliwością weryfikacji spełnienia wymagań.

20. Czy zamawiający jest zainteresowany jedynie modułem do nagrywania sesji czy też modułem do zarządzania hasłami i/lub kontami uprzywilejowanymi?

Odp. Zamawiający wymaga funkcjonalności nagrywania sesji oraz zarządzania kontami uprzywilejowanymi.

21. Czy zamawiający jest zainteresowany modułem AI do inteligentnej analizy nagrywanych sesji?

Odp. Zamawiający nie jest zainteresowany tą funkcjonalnością.

22. Czy system PAM ma być wyceniony per użytkownik systemu PAM czy per system IP?

Odp. Per system IP

23. Czy zamawiający korzysta już z jakiegoś systemu klasy PAM?

Odp. TAK

24. W ilu Data Center zamawiający chce wdrożyć system PAM. Czy Data Center są on-premise czy jest to private/public cloud?

Odp. Zamawiający preferuje instalację w dwóch DC ale dopuszcza instalację w jednym DC. Instalacje będą realizowane w DC on-premise.

25. Czy zamawiający dopuszcza wdrożenie systemu PAM w wersji nie mieszanej dla appliance tj. tylko appliance hardware lub tylko appliance virtual?

Odp. Zamawiający dopuszcza tylko jedno z tych rozwiązań.

26. Ile domen Active Directory ma obsługiwać system PAM?

Odp. Jedna domena AD

27. Ile połączeń RDP/SSH występuje dziennie u klienta?

Odp. 150-200 dziennie

28. Czy zamawiający chce zabezpieczyć dostęp do systemu PAM przez MFA? Jeśli tak to jakie?

Odp. Zamawiający posiada rozwiązanie MFA – Secfense. Jeśli będzie możliwość, to zdecydowanie z takiej możliwości skorzystamy

29. Czy w ramach nadmiarowości zamawiający dopuszcza zakup dodatkowego hardware appliance, który będzie offline, poza klastrem. W przypadku awarii jednego node'a z klastra, taki appliance mógłby być szybko podmieniony, bez zbędnego oczekiwania na wysyłkę od producenta?

Odp. Zamawiający nie dopuszcza zakupu nadmiarowego hardware appliance.

30. Pytanie dotyczące pkt. 1.4/2.11/4.14

1.4. Usługa wraz z opisem oferowanego rozwiązania powinna zapewniać śledzenie trwających sesji dostępu z poziomu przeglądarki internetowej i uniemożliwiać ryzyko zatarcia śladów niepożądanych działań, dokonanych przez zdalnych użytkowników;

2.11. Architektura Administrowanie, monitorowanie oraz podgląd sesji odbywa się poprzez przeglądarkę dedykowanej pojedynczej konsoli zarządzania.

4.14. W zakresie dodatkowej specyfikacji rozwiązanie powinno obejmować W rozwiązaniu podgląd monitorowanych sesji (zarówno "na żywo" jak i wcześniej nagranych) nie wymaga instalowania dodatkowego oprogramowania;

- Czy zamawiający dopuszcza rozwiązanie pozwalające na monitorowanie sesji za pomocą dedykowanego klienta systemu PAM? W oferowanym rozwiązaniu sesje archiwalne są możliwe do przeglądania za pomocą interfejsu WEB.

Odp. Zamawiający dopuszcza.

31. Pytanie dotyczące pkt. 4.12

4.12. Rozwiązanie pozwala na selektywne nagrywanie elementów sesji ;

- Czy Zamawiający dopuści zapis „Rozwiązanie pozwala na nagrywanie całych sesji”?

Odp. Zamawiający dopuszcza zapis.

32. Pytanie dotyczące pkt. 4.17

4.17. Dla protokołów RDP, VNC, SSH, TELNET, rozwiązanie pozwala na uzyskanie dostępu do grupy monitorowanych serwerów poprzez jeden adres sieciowy (jedną parę IP i port). Nazwa docelowego serwera jest wskazywana w nazwie użytkownika przy użyciu separatora, np. 'ssh -l user#mailserv nazwa-serwera';

- Prosimy o usunięcie zapisu, gdyż powoduje wykluczenie innych podmiotów oferujących system PAM i przekłada się na pogorszenie konkurencyjności oferowanych cen.

Odp.

Zamawiający wymaga:

„Dla protokołów RDP, VNC, SSH, TELNET, rozwiązanie pozwala na uzyskanie dostępu do grupy monitorowanych serwerów poprzez jeden adres sieciowy (jedną parę IP i port)”

lub

„Nazwa docelowego serwera jest wskazywana w nazwie użytkownika przy użyciu separatora, np. 'ssh -l user#mailserv nazwa-serwera';”.

33. Pytanie dotyczące pkt. 4.18

4.18. Rozwiązanie umożliwia tagowanie i komentowanie przeglądanych sesji;

- Prosimy o usunięcie zapisu, gdyż powoduje wykluczenie innych podmiotów oferujących system PAM i przekłada się na pogorszenie konkurencyjności oferowanych cen.

Odp. Zamawiający usuwa zapis.

34. Pytanie dotyczy:

4.20. Rozwiązanie umożliwia chwilowe wstrzymanie i wznowienie sesji;

- Prosimy o usunięcie zapisu, gdyż powoduje wykluczenie innych podmiotów oferujących system PAM i przekłada się na pogorszenie konkurencyjności oferowanych cen.

Odp. Zamawiający usuwa zapis.

35. Pytanie dotyczy:

4.21. Rozwiązanie umożliwia proaktywny monitoring, powodujący przerwanie sesji oraz alert do administratora po wykryciu zadanych komend lub ciągu znaków

- Czy zamawiający dopuści zapis istnienia proaktywnego monitoringu, bez automatycznych powiadomień?

Odp. Zamawiający dopuszcza zapis.

36. Pytanie dotyczy:

4.22. Rozwiązanie umożliwia kontekstowe przeszukiwanie zachowanej sesji.

- Czy zamawiający dopuszcza rozwiązanie pozwalające na wyszukiwanie wpisywanych znaków z klawiatury w sesjach terminalowych SSH?

Odp. Zamawiający dopuszcza takie rozwiązanie.

37. Pytanie dotyczy:

4.23. Rozwiązanie umożliwia wyszukiwania tekstu w sesjach graficznych (np. RDP);

- Czy zamawiający dopuszcza rozwiązanie pozwalające na wyszukiwanie w sesjach RDP nazw otwieranych okien (aplikacji)?

Odp. Zamawiający dopuszcza takie rozwiązanie.

38. Pytanie dotyczy:

4.24. Rozwiązanie umożliwia dołączenie się administratora do sesji telnet, SSH, RDP, VNC z poziomu przeglądarki (np. dla wprowadzenia hasła, wpisanie polecenia systemowego);

- Czy zamawiający dopuszcza rozwiązanie pozwalające na dołączanie do sesji za pomocą dedykowanego twardego klienta?

Odp. Zamawiający dopuszcza.

39. Pytanie dotyczy:

4.25. Rozwiązanie ma możliwość monitorowania, raportowania oraz analizy aktywności użytkownika podczas sesji (np. dla oceny produktywności i/lub kontroli stopnia zaangażowania i rozliczeń z firmą zewnętrzną);

- Czy Zamawiający może potraktować funkcjonalność na temat możliwości aktywności użytkownika w trakcie sesji jako opcjonalną?

Odp. Zamawiający dopuszcza takie rozwiązanie.

40. Pytanie dotyczy:

4.26. Rozwiązanie pozwala na współpracę z rozwiązaniem Microsoft RD Connection Broker

- Prosimy o usunięcie zapisu, gdyż wskazuje na jednego dostawcę rozwiązania.

Odp. Rozwiązanie musi pozwalać na korzystanie ze wszystkich funkcjonalności protokołu RDP.

41. Pytanie dotyczy:

4.33 System PAM musi zapewniać szyfrowanie kopii bezpieczeństwa systemu, przy czym siła szyfrowania musi być na poziomie AES-256 ;

- Czy zamawiający dopuszcza system PAM, który szyfruje kopię zapasową w części gdzie znajdują się hasła z magazynu haseł (konfiguracja systemu jest pozostawiona bez szyfrowania)?

Odp. Zamawiający usuwa zapis.

42. Pytanie dotyczy:

5.9. System powinien umożliwiać tworzenie dedykowanych raportów; Object count: 499ów;

- Czy zamawiający dopuszcza rozwiązanie z predefiniowanymi raportami z filtrowaniem?

Odp. Zamawiający dopuszcza.